

**THIS DOCUMENT IS NOT A CONTRACT OF EMPLOYMENT. PRIOR DOCUMENTS ON THIS SUBJECT ARE REVOKED. EMPLOYMENT WITH THE CITY OF GREENVILLE IS AT-WILL.**

## CITY OF GREENVILLE

POLICY NO.: HR-30

DATE: September 15, 2010

SUBJECT: City Technology Usage Policy

### CONTENTS

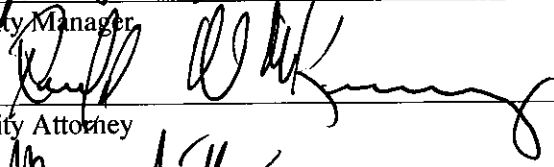
- I. Purpose
- II. Applicability
- III. Definitions
- IV. Policy
- V. Procedures
  - A. City Technology Operating Standards
  - B. Acquisition of Technology Resources
  - C. Internet and Email Access and Usage
  - D. Incidental Personal Use of Internet and Email Systems
  - E. Security, Storage, and Protection
  - F. Changes in Employee Status
  - G. Technology Usage Monitoring and Reporting
  - H. Investigation of Illegal, Excessive, or Unauthorized Internet and Email Usage
  - I. Enforcement
  - J. Exceptions
  - K. Roles and Responsibilities

#### Exhibit

- A: Email Graphic Design Standards
- B: Receipt of City Technology Usage Policy

APPROVALS:

  
\_\_\_\_\_  
City Manager

  
\_\_\_\_\_  
City Attorney

  
\_\_\_\_\_  
Human Resources Director

## **I. Purpose**

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at the City of Greenville in order to safeguard and protect all technology resources.

## **II. Applicability**

This policy applies to all employees, contractors, part-time employees, temporary staff, volunteers, interns, and other individuals who are granted access to City of Greenville's computer services (hereinafter called "computer users" or "users").

## **III. Definitions**

- **Computer System:** Includes individual desktop computers (PCs), mobile data terminals, mail system, Internet access, laptop computers, storage media of any kind, file servers, and all other components of the City's computer network.
- **City-owned Technology Resources:** Technology resources paid for by City funds, including but not limited to: electronic and communications equipment, software, and systems, including but not limited to computers, computer networks, software, copiers, scanners, printers, other computer peripherals, telephones, cellular phones, radios, applications such as the Internet, e-mail, office systems, and other equipment or other property or resources under the City official's or employee's official control or direction or in his or her custody or to which he or she has access.
- **Data files:** Information contained in files such as e-mail messages, text message logs, database tables, telephone records, extracts from databases, or output from applications.
- **Device:** Any piece of equipment attached to a computer in order to expand its functionality. Some of the more common peripheral devices are printers, scanners, disk drives, tape drives, microphones, speakers, cameras, etc. For purposes of this policy, the word device also includes removable devices such as Universal Serial Bus (USB) devices, cell phones, etc.
- **Digital Equipment:** Includes but is not limited to computers, laptops, mobile data terminals, pagers, telephones, cellular phones, Personal Digital Assistants (PDAs), and combination devices such as Blackberries. Any technology provided by the City for communications, computing, printing, etc. is covered by this definition.
- **E-mail:** The City's electronic mail system.
- **Freedom of Information Act (FOIA):** FOIA is a law ensuring public access to Government records, including those of the City of Greenville. FOIA carries a presumption of disclosure; the burden is on the government - not the public - to substantiate why information may not be released. Upon written request, the City is required to disclose those records, unless they can be lawfully withheld from disclosure under one of the specific exemptions in the FOIA.

- **Hacking/Hacking Tools:** Behavior and tools designed to circumvent security measures, or to otherwise effect unauthorized changes to computer hardware and software.
- **Intranet:** Web site containing content for internal use.
- **Internet:** The Internet is a worldwide “network of networks,” including bulletin boards, World Wide Web (WWW), data servers, applications, messaging services, and other functions and features, which can be accessed via computer, a Blackberry, or other devices.
- **Personal Identifying Information:** This information includes first and last name (or first initial) with any combination of Social Security number, driver’s license number, financial account number or credit card or debit card number in combination with any required security code and other identifying information such as date of birth, address, or telephone number that would allow a person’s identity or information to be compromised.
- **Removable Device:** Any storage device that can be removed from a computer, laptop or network with or without administrative privileges to the device. Examples include but are not limited to: removable hard drives, ipods, cameras, memory cards, thumb/flash drives, hot swappable CD/DVD drives, etc.
- **Social Networking:** Any Internet site that is focused on creating “networks” of individuals such as My Space, Face Book, LinkedIn, etc.
- **Streaming Audio:** Technology used to “play” audio/video on a PC over a network. Can be used for music, voice, lectures and other audio/video material. It generally consists of a continuous stream of data coming from a network.
- **Users:** Include but are not limited to full time and part-time employees, council members; full and part-time employees, contractors, temporary employees, volunteers, interns, and other individuals who are granted access to City computer services.
- **Web Browsing:** Use of a browser tool to access Web sites on the Internet.

## II. Policy

This policy defines the oversight, use and protection of the City of Greenville’s computing equipment, network, voice, electronic communication and data repositories. This policy also specifies the proper utilization of email and Internet access as well as the computer facilities and services ("hardware" and "software") owned or leased by the City of Greenville (the City), or otherwise licensed to the City, through which email and Internet access is accomplished (hereinafter called "computer services"). These facilities include, but are not limited to: PCs (personal computers), all components inside a PC, all components connected to a PC, monitors, printers, display stations, servers, telephones, hubs, switches, routers, cabling, mobile data terminals, personal digital assistants and handheld computers (operating as a stand-alone system or connected through a wired or wireless network), all software applications and operating systems, all data, all data lines, all phone lines, wireless communications devices, etc. and all files prepared by City employees or received by City employees when using the City's computer services.

This policy applies to all employees, contractors, volunteers, and other individuals who are granted access to City of Greenville's computer services (hereinafter called "computer users" or "users"). It is intended to ensure that all City computer users understand their responsibilities in regards to proper usage of the City's computer services. The City's computer services are made available to users for City business and are not provided for the purpose of facilitating private or personal communications or file preparation. Use of the City's computer services is not an entitlement. It is a business tool which carries with it responsibilities.

Employees entrusted with the use of the City's computer services must be held accountable for the proper use of the facilities. All users granted access privileges with City of Greenville computer services are required to comply with this policy. This policy must be read in conjunction with other City policies including, but not limited to, those regarding City communications, confidentiality, solicitation, harassment, discrimination, etc.

## **V. Procedures**

### **A. City Technology Operating Standards**

City Information Technology Services (CITS) division is authorized to set prudent operating standards and to make periodic adjustments in operating procedures for computer services, as needed to maximize system capacity, security and performance. CITS will publicize such adjustments via email and by other means. Users are expected to comply with periodic CITS advice and directives related to computer services, such as avoiding Internet websites and applications that overtax City computer services, archiving historical emails, and removing emails with large-size file attachments.

CITS will educate Internet and email system users to avoid practices that violate City policy or applicable local, State, and Federal law or which will detract from system performance.

### **B. Acquisition of Technology Resources**

City Information Technology Services (CITS) division must evaluate and approve specification, acquisition and acceptance of all software, hardware (permanent or removable devices), technology related services (installation, configuration, programming) and related maintenance and support contracts, whether the selected products or solution will be on the network or off or used by one or many people, and for all program and project funding sources. In addition, acquisition of technology resources should conform to existing purchasing policies and procedures as outlined in OMB policies.

Most City-owned technology has a pre-determined lifecycle replacement period and must be surrendered for replacement on a one-on-one basis or retired, according to that schedule. Such technology may not be redeployed or otherwise put back into use without approval from CITS. Nor may such computer equipment and devices be sold, conveyed, lent, disposed of, or retained for personal use, except in accordance with standard CITS procedures.

### **C. Internet and Email Access and Usage**

Internet and email access is provided to City users to facilitate and expedite communications and research necessary for the conduct of City business. The City encourages the use of email and Internet access for that purpose. The computer services needed to provide email and Internet access represent a considerable financial commitment by the City for telecommunications, networking, software, storage, support, etc. The City intends for this tool to be used in a responsible, ethical, professional, and legal manner, consistent with the City's business needs.

1. Compliance with Applicable Laws and City Policy. Internet and email use must comply with applicable laws and City policies including but not limited to all Federal and State laws, and City policies governing sexual harassment, discrimination, and intellectual property protection, privacy, public disclosure, and confidentiality, misuse of City resources, information and data security. All users have a fiduciary and professional responsibility to the City to use internet, intranet, email, and text messaging properly in accordance with this policy.
2. No Expectation of Privacy. The City reserves the right to inspect any and all files stored on computer facilities at any time in order to assure compliance with this policy and all other policies that involve practices that are directly or indirectly associated with internet usage. This right applies to all work-related equipment, devices, and software. All personal uses intended to be private should not use City software, equipment, or devices. Computer users can have no reasonable expectation of privacy in using the City's computer services in the transmission and receipt of Internet information and email messages. All data and messages originating from, received at, or transmitted through the City's computer services are the property of the City of Greenville. An employee's rights while using the Internet via City resources does not include the right to privacy.

The City has the right to access or monitor email messages for work-related purposes, security, or to respond to public record requests. Email messages—sent or received—are considered business records which are subject to discovery in administrative, judicial, and other legal proceedings. Email messages sent or received in the conduct of City business are not confidential unless they qualify for non-disclosure under the Freedom of Information Act (FOIA) and then only to the extent permitted under FOIA. Email messages whether sent or received are subject to requests for information from any member of the public under FOIA. Users shall have no expectation of privacy in email messages, whether they are business related or an allowed personal use as provided herein. Nothing in this provision shall be construed as creating a right of public access for media or members of the public that does not otherwise exist under the FOIA or other provisions of law.

These provisions on the limitations on expectation of privacy are intended to comply with decisions rendered by the United States Supreme Court addressing reasonable search and search seizure process in the governmental work place under the Fourth Amendment to the Constitution of the United States and comparable provisions under South Carolina law. The authority of the City to monitor, inspect, and secure information and things shall be construed to be vested to the maximum extent permitted by those provisions of law. Nothing herein shall be construed to allow arbitrary or capricious inspection of personal information on communication for non work-related purposes. Any provisions contained herein that does not

so comply with applicable provisions under the Fourth Amendment and comparable provisions of state law shall be severable from the remainder, so the remainder is given full force and effect.

All messages should be composed with the expectation that they may be shared with the public or may be subject to review in determining what a public document is. Use of City's email and text messaging devices shall be considered consent to City officials, managers and other employees to inspect, use, or disclose any email or other electronic communications and/or data without further notice. Due to public record laws, use of any other email system to conduct City-related correspondence is not advised.

3. Privileged Communications. Messages received from the City Attorney or Assistant City Attorneys, or private attorneys acting on behalf of the City, its officials or employees, may be privileged communications and therefore, confidential, and these messages shall not be forwarded to non-City persons without prior approval of the an attorney in the City

Attorney's Office. Confidential material must not be sent via email. Email messages may be intercepted, viewed, and used for non-approved purposes, especially over the Internet, a medium over which the City cannot control.

4. Managing Email Storage and Retention. As discussed, email is considered part of the public record and is subject to disclosure under the FOIA. Managing individual email storage and retention is the responsibility of each individual, consistent with the City's document and records-retention guidelines.
5. Personal Email Accounts and Personal Email Devices. Direct access to personal email and associated programs may not be set up on City devices. These devices include desktop PCs, laptops, Smartphones, and Blackberries. Occasional access to personal web-based email from City devices is permitted. This provision does not preclude isolated instances of obtaining brief access to a personal account, subject to the conditions of subsection D below, for matters needing urgent attention.

Personal devices (i.e., Blackberry or Smartphones) may not be configured and connected to the City's email system except for special circumstances and only with Department Director and CITS approval. Under certain circumstances, it may be permissible for an employee to set up an email rule from their City email account to forward copies of their City business emails to a personal email account.

6. Email Graphic Standards. Email presents an opportunity to provide a unified and cohesive image to the community. Standardizing the overall look of email helps convey professionalism and maintain our identity as a City government. To ensure that all emails from City of Greenville employees reflect a professional appearance, employees must and adhere to the City's graphic standards. Exhibit A summarizes the guidelines specific to emails.

#### **D. Incidental Personal Use of Internet and Email Systems**

The City's technology resources, including email and Internet web browser, are City property and intended for use to conduct City business by its authorized users. Limited personal use is permitted under specific circumstances.

1. Permissible Use. Subject to the mandates and objectives of this policy, brief personal use of Internet and email systems is permitted if it does not:
  - a. Interfere with one's work or anyone else's work at the City;
  - b. Result in a cost to the City;
  - c. Distract from the conduct of City business;
  - d. Compromise the security or integrity of City information or software;
  - e. Have a harmful effect on the performance of City computer services, such as when Internet browsers and applications are left open for extended periods of time or when software unrelated to City business is downloaded;
  - f. Violate or infringe upon the right of any other person or entity in the lawful exercise of their rights and duties;
  - g. Constitute a criminal offense or give rise to civil liability; or
  - h. Violate a City policy or regulation.
2. Prohibited Use. Inappropriate use of the City email system and Internet access is prohibited. **Systematic and pervasive use of email or Internet systems for non-job-related purposes is strictly prohibited.** Inappropriate uses include, but are not limited to the following:
  - a. Using the City's computer services in any way prohibited by City of Greenville policies or procedures.
  - b. Committing any crime using the Internet or making threats against other persons or institutions.
  - c. Using obscene or pornographic language, pictures, or drawings in outgoing mail or willfully receiving files containing obscene or pornographic language, pictures, or drawings, regardless of whether such files are downloaded, except for police officers working on a criminal case where such information is related to that criminal case. Attachments to email messages containing such language or pictures are also prohibited.
  - d. Using inappropriate language or subject matter. Electronic exchanges that occur in the course of conducting City business will be considered a communication of the City and will be held to the same standards as formal letters. Content and images posted in the City's Intranet, Internet FTP, Social Media sites or sent via Twitter should be consistent with the City's policies and practices. City policies, including policies prohibiting discrimination and sexual harassment, shall apply to the use of e-mail. E-mail shall not be used for the expression of unlawful or discriminatory ill will or bias against individuals or groups, offensive materials such as obscenity, vulgarity, or profanity, or other non-business like material. Sexually explicitly material, cursing and name-calling are expressly prohibited.

- e. Downloading files in such a way as to avoid copyright infringement. All information that is posted, copied, or shared, either on the City's Intranet, servers, and desktops or on the City's Internet or Social Media sites, must be done in accordance with the laws that governing copyrighted materials including, but not limited to, photographs, magazines, books, copyrighted music, the installation of copyrighted software for which the City or end user does not have an active license, or the installation of "pirated" software.
- f. Mounting an attack on the security of any system, including attempts to hack into or to introduce or spread viruses through a system. Any unauthorized or deliberate action that damages or disrupts a computer system, or causes it to malfunction.
- g. Sharing email and Internet passwords, or gaining access without permission to another employee's email or Internet access. Deleting, examining, copying, or modifying files or data belonging to other users without proper authorization. Reading or sharing information via the email system without proper authorization.
- h. Misrepresenting one's identity in any way on the Internet (via news groups, chat rooms, blogs, etc.) or email, including the sending of falsified messages.
- i. Using email for mass mailing. The City's email system is not intended to be used for general mass mailings to all City employees. The citywide email distribution list should be used for critical and time-sensitive, City business information only. Mass mailings that contain attachments utilize a large amount of disk space. The City uses other electronic publications to communicate information that are more efficient and cost-effective. Effort should be made to restrict unnecessary e-mail traffic, including minimizing the size of attachment files, and using network drives instead of large distribution lists to share file attachments with large groups.
- j. Broadcasting unsolicited messages to internal or external email addresses, unless authorized by a division or Department Director as a means of official notice for City business. Broadcasting or forwarding unsolicited pyramid or chain email is also prohibited.
- k. Attempting to alter or bypass the City's filtering mechanisms. Filtering software will be actively used by the City to preclude access to inappropriate web sites unless specific exemptions are granted as a requirement of work duties (e.g., police have the ability to access sites on criminal activity, weapons etc.). See Section G for additional information on granting exceptions.
- l. Participating in online publishing activities or in online discussion groups that are not work related.
- m. Developing web or home pages for personal use.
- n. Loading and accessing personal Internet provider accounts (e.g., America On Line, etc.).
- o. Offering personal products or services for sale, soliciting for outside business ventures, personal parties, membership in any organization, political causes, religious causes, social causes, soliciting funds for charities without approval or other matters not connected to the City's business.
- p. Posting to or buying from online auction or sales sites unless specifically job related and approved by management.



- q. Using email in lieu of an employee's responsibility to contact his/her immediate supervisor directly for the purpose of reporting that an individual is unable to work on a given day.

#### **E. Security, Storage, and Protection**

Effective security requires the participation and support of every user in the organization. The City employs enterprise tools to manage, monitor, and protect the organization from internal and external security threats and data loss. In addition to these measures, it is the responsibility of individuals to remain vigilant in their awareness and protection of the City's resources, including equipment and data they have access to and while in their possession. Specific due diligence requirements are outlined below:

1. Remote Access to City Computer Network. Remote access to the City network is permissible by use of Virtual Private Network (VPN) capabilities. VPN provides access to files stored by a user computer from a remote device such as a personal home computer or City issued laptop. Remote VPN access must be configured by CITS and will only be granted based on a legitimate business need and approval by the requesting users' Department Director. On an annual basis, CITS will produce a report of users with VPN access for Department Directors review. Remote access to City email is also available to all City employees through web mail and does not require the use of VPN or Department Director approval.
2. Password-Protect Access to Computer Services. Users of City owned computer services are personally responsible and accountable for all material received and sent through their accounts or user identification, including mail, data, documents, and software. Thus, users are encouraged to password-protect access to computer services while absent from their work area during normal business hours. City devices and computer equipment must be logged out or "locked" when unattended for extended periods of time. As a standard practice, CITS will enable screen saver and password protect options for systems left idle for more than 30 minutes. Exceptions to this policy for attended customer service or public safety needs will be granted as needed.
3. Logging off after Normal Business Hours. After normal business hours, computers must be logged out to avoid unauthorized persons from accessing the computer. (The purpose of this provision is to protect official information from unauthorized or premature inspection in those instances when policies, practices, and programs are in a developmental stage; when personnel information is under review; when investigations are underway; when proprietary information has been transmitted, prepared or assessed; or, in other like circumstances requiring the orderly preparation and transmission of information.)
4. No Sharing of User Accounts and Passwords. User accounts and passwords may not be shared. The individual logged onto the City network must be present while logon credentials are being used to access network resources. In general, it is not permissible to download "personal information" to any removable/portable device, including your laptop computers, unless access to that information is within the scope of your job, your manager has approved the copy of information to a portable device, and the data or device is "encrypted."
5. Enabling Maintenance and Security Updates. All users must log off of their PC and leave it powered on at the end of their shift to enable off-shift maintenance and security updates.

6. Protecting Personal Information. Leaving personal, sensitive or confidential information exposed to view while unattended, either on paper or on screen, is prohibited. It is the responsibility of each individual to prevent unauthorized and indiscriminate access to “personal information” that could pose the threat of identity theft, thus risking a person’s privacy, financial security and other interest.
7. Unattended Non-business Related Web Pages/Applications. Users must refrain from leaving non-business related web pages open and unattended for extended period of time and to refrain from accessing Internet websites or applications which consume large amounts of computer resources. Such applications include streaming video and audio.
8. Ensuring System /Network Security. Intruding or attempting to intrude into any gap in system or network security is prohibited. Sharing of information with others that facilitates their unauthorized access to the City’s data, network or devices, or their exploitation of a security gap is also prohibited.
9. Removable Devices. Removable devices such as USB drives and PDA/handhelds/smart phones, cameras, etc. must always be password enabled. Whenever possible, laptop and desktop hard drives and removable devices should only contain copies of source files not the original files.
10. Transmitting Confidential Data. Transmitting confidential data in part or full via e-mail or other unencrypted medium is prohibited.
11. Reporting Lost, Stolen, or Damaged Equipment, Software or Data. Individuals must report to the City any equipment, software or data that is lost, damaged or stolen at their first available opportunity. Reports will be made to a supervisor, manager or department director. Lost equipment, especially that containing sensitive or confidential information as defined here, must be reported immediately to CITS. Stolen computers, laptops, Personal Digital Assistant’s (PDA) and cell phones must be reported immediately to CITS or the local police department. Unrecoverable equipment may incur additional replacement costs to individuals or departments.
12. Using Anti-virus Software. The possibility of downloading a file with a computer virus is great and care must be taken not to contaminate any computers in the City. Users of computer services must understand that email is the preferred vehicle with which lawbreakers transmit destructive viruses, and thus users must use extreme caution when opening email attachments, even when email attachments come from trusted sources. Any computer user who receives a suspicious email attachment should not open the attachment, but should delete the email or contact the Help Desk for assistance.

Employees must use City provided anti-virus software and scanning tools regularly to scan material from removable devices prior to use. Files copied from an Internet site, or outside source, must be scanned by virus checking software prior to being used on a City computer. CITS shall make options available for virus checking of copied files.

13. Storage of any Copyrighted Material. Storage of any copyrighted material on a network server or local hard drive including, but not limited to photographs from magazines, books or other copyrighted sources, copyrighted music, the installation of any copyrighted software for which the City or end user does not have an active license, or the installation of “pirated” software is strictly prohibited.

14. Use of Email "Delete" Function. Users must understand that the use of the email "delete" function does not immediately remove the targeted message from the City's email server. Messages deleted from the email system may still be available to others, either through a system backup or from all recipients of the message.

#### **F. Changes in Employee Status**

1. Notification of Employee Status Changes. The Human Resources department will notify designated person(s) in CITS of employee status changes that require removal of Internet and email privileges for the affected person.
2. Right to the Content of Discontinued Employee's Email messages. If the employment of any user is discontinued, that user has no rights to the content of his/her email messages unless authorized by the Division head, Department Director or City Manager. The person will not be allowed further access to the City email system. Thus, a change in employment status may cause an individual to lose authorization to the City email system. Changes in employment status include, but are not limited to: resignation, retirement, termination, reassignment, promotion, demotion, or a loss of authorized user status. If a change in employment status occurs, CITS will only delete an individual's email after receiving approval of the employee's Department Director.
3. Access to Employee Computer during Absences, Transfers or Termination. Department Directors or their designees may request and be granted access to an employee's computer account if the employee is on leave of absence or vacation, is transferred or terminated, or any time when there is a valid business justification.

#### **G. Technology Usage Monitoring and Reporting**

1. Right to Inspect and Monitor Technology Usage. The City reserves the right to monitor and record all messages of all City computer services. As discussed in Section B.2., there is no right or expectation to privacy in the course of using the City's technology resources, whether conducting City business or for incidental personal use. All data and messages originating from, received at, or transmitted through the City's computer services are the property of the City of Greenville. Examples include: email, voice mail, text message logs, Internet logs, computers, laptops, handhelds, etc. Such records may be subject to disclosure under FOIA or hereinafter amended or may be disclosed for audit or other legitimate City operational or management purposes. Pursuant to this Subsection (G), the City may conduct requested audits in order to ensure compliance with its policies and requirements, to respond to public disclosure requests, investigate suspicious activities or security threats, or to fulfill legally mandated requirements (i.e., software license rules, Payment Card Industry regulations, and the Health Insurance Portability and Accountability Act (HIPPA) requirements.)

The City uses security software that is capable of recording each and every Internet website visit, each chat, newsgroup, text message, or email message, and each file transfer into and out of the City's internal networks, and the City reserves the right to utilize this software at any time. The City's security software can record Internet activity and analyze usage patterns.

2. Internet Content Filtering. As standard practice, the City restricts user access to specific categories and types of internet sites and content through the use of an internet filter. This practice includes all City computer resources regardless of method of accessing the Internet:
  - a. *Default Blocked Content Categories:* Adult/Sexually Explicit, Advertisements & Popups, Alcohol & Tobacco, Criminal Activity, Gambling, Games, Hacking, Illegal Drugs, Intimate Apparel & Swimwear, Intolerance & Hate, Peer-to-Peer, Personals & Dating, Proxies & Translators, Ringtones/Mobile Phone Downloads, Sex Educations, Streaming Media, Suspect / Threat URLs, Tasteless & Offensive, Violence, Weapons.
  - b. *Granting Exceptions:* Exceptions to blocked content are permitted provided there is a business related need and approval is granted by the requesting users' Department Director. The exception process requires submission of an exception request to CITS. Exceptions typically are granted by content category however individual sites can be unblocked for specific URL's.
  - c. *Exceptions Reporting:* The CITS Server Administrator will maintain current documentation on all filtering exceptions. On an annual basis, CITS will produce a report for Department Directors listing users within their domain who are currently granted filtering exceptions. Continuation of exceptions will be dependent upon timely confirmation of the annual report at the Department Director level.
3. Technology Usage Reporting. The City has empowered CITS to produce generalized and specific activity reports on system usage.
  - a. *Routine Generalized Reporting:* On a quarterly basis, the CITS Server Administrator will produce a set of standard comparative charts and reports for each division within the City indicating internet activity by staff. High levels of activity in comparison to other division staff may serve as an indication of potential Internet abuse provided their job responsibilities do not require a high level of internet usage in the performance of their job. The standard report formats will be developed in conjunction with input from Department Directors to assure usability and ease of interpretation. These routine reports will be delivered directly to each Department Director for review and distribution within their department.
  - b. *User Specific Investigative Reporting:* As discussed in Section H below, investigating specific user activity can only be initiated by Department Directors through the Human Resources Director. The Human Resources Director will communicate directly with the CITS System Administrator regarding the details of what needs to be investigated. Investigation details are to be strictly confidential. For workload accountability purposes, the CITS IT Manager should be informed that the Server Administrator is assisting in an investigation but not privileged to the details of the investigation.

#### **H. Investigation of Illegal, Excessive, or Unauthorized Internet and Email Usage**

The following steps will be taken when there is a reasonable basis to suspect that an employee is violating this policy:

1. If CITS, during the course of routine maintenance and trouble shooting activities detects Internet, messaging, or email activity that appears to violate local, State or Federal law, a written report of such suspected activity will be provided to the Human Resources Director and to the Police Chief or his/her designee. A copy of the written report will also be provided to the City Manager by the Human Resources Director.

The Human Resources Director and designated persons in the Police Department are responsible for further investigation and follow-up on reported Internet and email activity that appears to be illegal. CITS staff will cooperate with the investigation by providing required data and maintain strict confidentiality of such knowledge and activity.

2. If, through its routine maintenance and problem solving activities, CITS personnel identifies reasonable evidence or suspected patterns of excessive and unauthorized activity, such should be immediately reported to the CITS IT Manager. The IT Manager will then provide a written report of the activity directly to the Human Resources Director and the Department Director of the person and/or groups of employees whose computer and network login is associated with the activity in question. The Human Resources Director will work in collaboration with the impacted Department Director to investigate the matter and determine the appropriate course of any required disciplinary action. CITS staff will cooperate with the investigation by providing required data and maintaining strict confidentiality of such knowledge and activity.
3. Circumstances may warrant the need for City management to request that the Internet and email system usage by an individual employee and/or groups of employees be monitored for non-compliance with City policies and procedures. In making such a request, a reasonable basis for suspecting illegal, inappropriate, or excessive use of the Internet or email must be provided with the request at the time the request is submitted.
4. If the supervisor of the employee or group of employees has a reasonable basis for requesting a usage report, he/she must submit the request to his or her Department Director for review. If the Department Director concurs with the request, the request should be submitted to the Human Resources Director for review and approval. If the Department Director is the source of the problem, condones the problem, or ignores the problem, then the requesting supervisor/manager should contact the Human Resources Director.

The Human Resources Director will coordinate the request directly with the CITS Systems Administrator for processing reports. The resultant report will be submitted to the requesting Department Director and the Human Resources Director for review. Any necessary follow-up and/or disciplinary action will need to be coordinated with the Human Resources Director.

If the Human Resources Director is the source of the problem, then the request should be submitted to the City Manager for approval. The City Manager will forward the approved request to the CITS Server Administrator for processing. If the City Attorney is the source of the problem, then the request should be submitted to the City Manager for approval. If the City Manager is the problem then the request should be submitted to the City Attorney for approval.

The City Manager, City Attorney, and/or Human Resources Director may request CITS to

monitor and provide reports on Internet and email system usage by individuals or groups of employees in any department as circumstances warrant.

## **I. Enforcement**

In order to safeguard City resources, violators of this policy will be subject to disciplinary action up to and including termination. Disciplinary action may include, but is not limited to, loss of Internet access and email privileges, probation, suspension, termination of employment and/or civil or criminal penalties. In the event possible illegal activity is discovered, the City will cooperate with any legitimate law enforcement authority.

## **J. Exceptions**

Exceptions to this policy may be granted on a case-by-case basis, upon request by Department Director and approval by the City Manager. Exceptions to this policy must be submitted to the Human Resources Director and OMB Director in writing for processing.

## **K. Roles and Responsibilities**

### **1. OMB/CITS Responsibilities**

- Establish and communicate operating standards and procedures for computer services.
- Maintain the security and reliability of all network servers and the data contained in them. This will be accomplished, at the discretion of CITS, with daily backups of all network servers. Such data will be secured in an area designed for protection from theft and fire, etc. and be removed from the physical backup area.
- Keep the City's networks operational 24 hours a day, seven days a week, with the exception of the scheduled maintenance window.
- Coordinate the installation and maintenance of all City owned hardware and software and ensure that "outside connection" will not impact other City networks.
- Educate Internet and email system users to avoid practices that violate City policy or applicable local, State or Federal law or which will detract from Internet connection performance.
- Provide Department Directors with quarterly standardized comparative internet usage reports.
- Support Human Resources Director in the conduct of employee investigations related to illegal, unauthorized, and excessive Internet and email usage.
- Maintain confidentiality of any technology usage investigation.

2. Management Responsibilities

- Distribute this policy to all affected department employees and ensure that they participate in training on this policy.
- Obtain a signed copy of the Receipt of City Technology Usage Policy (Exhibit B).
- Enforce compliance with the policy.
- Review and distribute quarterly comparative internet usage reports provided by CITS and conduct any necessary follow-up.
- Review and make decisions regarding the approval of all non-work related broadcast announcements. Acceptable uses for non-work related broadcast announcements would include arrival or departure of a department employee or an approved charitable campaign event.
- Review and process approved Internet Filtering Exceptions to CITS; provide annual review and confirmation of exceptions report provided by CITS.

3. Employee Responsibilities

- Cooperate with CITS with system maintenance by making system available for access in conducting repairs and maintenance.
- Comply with the standards/requirements outlined in this policy including network and file storage procedures.
- Monitor personal use of the Internet, messaging, and other applications, to ensure that the City is being appropriately served.
- Obtain authorization from their supervisor before incurring charges; for example, downloading data or accessing a paid service.
- The employee will be responsible for the backup and security of non-network (i.e. C:/ drive) data on their assigned workstation.
- Request Desk Service (ext. 4444) to download and install software unless expressed consent from CITS has been granted for employees to download and install software.



## **Email Graphic Standards/Guidelines**

To ensure that all emails from City of Greenville employees reflect a professional appearance and adhere to the City's graphic standards, the following guidelines have been established by Public Information and Events:

1. When composing a new email, select black as the default text color for the body of your email. A dark color such as blue or black should also be used when replying back to an email. To adjust the default for your font type, size and color, go to Tools>Options and select the "Mail Format" tab. Click on the button labeled "Fonts" and make your selections.
2. Fonts that are easily readable should be chosen as the default font. Script or italicized fonts tend to be difficult to read and should be avoided. Examples of preferred fonts include Arial, Times New Roman and Courier New.
3. The background of your email should be free of patterns or distracting colors. In Outlook, the background is called "Stationary." To adjust your stationary, go to Tools>Options and select the "Mail Format" tab. In the center of the page, under "Use this Stationary by Default," choose "None."
4. Email signatures have been designed to showcase the City's logo and establish a professional appearance and structure for emails. You may use this optional City Signature or a simple text signature. Please contact the Help Desk at 467-4444 for assistance in setting up a City Signature.
5. Any additional information included with your email signature is a direct reflection of the City. Only information that is professional in nature is permitted and should be listed below the email signature in the same size or smaller type size.





**EXHIBIT B**

**City of Greenville  
Receipt of City Technology Usage Policy**

The City of Greenville has developed safety and work rules for the well being of employees, the public and our customers. Attached is a copy of the City of Greenville's City Technology Policy. I, \_\_\_\_\_ (print), have been given a copy of the policy to read and become familiar with its requirements, even before any additional training on this subject occurs.

**EMPLOYEE ACKNOWLEDGEMENT:**

I understand the above and will review this policy promptly and if I have questions before I complete training I will ask my supervisor to contact the Human Resources Director and my questions will be answered.

I hereby acknowledge receipt of a copy of the City of Technology Usage Policy. I will review it promptly and understand that my continued employment is dependent upon my following these rules and all policies and rules of the City of Greenville.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
Date

\_\_\_\_\_  
Authorized Representative

\_\_\_\_\_/\_\_\_\_\_/\_\_\_\_\_  
Date